PCT/IB03/04563

IB/03/4563

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

02293224.8

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Anmeldung Nr:
Application no.: 02293224.8
Demande no:

Anmeldetag:
Date of filing: 23.12.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

SCHLUMBERGER Systèmes
50, avenue Jean Jaurès
92120 Montrouge
FRANCE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Retention of old mobile number on SIM card replacement

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

EP/17.10.02/EP 02292574

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04Q7/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SI SK

Retention of old mobile number on SIM card replacement

Technical field

This invention relates, in general, to a communication system (and architecture thereof) and is particularly, but not exclusively, applicable to the management of the association of International Mobile Subscriber Identities (IMSIs) and Mobile Subscriber Integrated Service Digital Network (MSISDN) numbers for a cellular communication system architecture.

The solution described in the following sections is targeted at improving the GSM activation process in cases where an existing GSM subscriber seeks to replace his / her SIM card, but wishes to retain his / her old mobile number.

Prior Art

A mobile number (MSISDN) is assigned to a SIM card (IMSI and Ki) in various elements of a GSM network. These network elements include, among others – Authentication Centre (AuC), Customer Care & Billing System (CCBS), Home Location Register (HLR), Mobile Switching Centre (MSC).

If an existing subscriber (say $MSISDN_A$, $IMSI_A$, Ki_A) seeks a SIM card replacement and at the same time wishes to retain his old mobile number, the new card details (say $IMSI_B$, Ki_B) have to be assigned to his old number ($MSISDN_A$). This re-assignment has to be done on all network elements where the combination $MSISDN_A$ - $IMSI_A$, Ki_A is defined.

At times this is simply not possible, since various network elements have pre-defined ranges, and fixed combinations of MSISDN – IMSI pairs. Even when re-assignment of old number is possible, the old card details ($IMSI_A$, Ki_A) are left

unused on the system, and have to go through a tedious quarantine process before they can be recycled again (ie, used to personalise another SIM card). Needless to say, presently, re-assignment of old mobile number to a new SIM card is a cumbersome process involving manual intervention & processes on the part of the GSM operator. These manual processes imply wastage of effort, time and money. For the end user, the present process is inconvenient, as several manual checks have to be applied.

Summary of the Invention

The proposed solution seeks to facilitate retention of old number (in case of SIM card replacement), by performing Over The Air changes on the SIM card(s), and by removing the need to do any changes on various network elements.

To achieve this objective, according to the invention, the management of the phone numbers is performed according the following steps:

- A service-inserting step, in which the subscriber is required to insert his / her new smart card containing at least one parameter attached to the second phone number;
- A service-replacing step, in which the application server sends a message (M2) for replacing, in the new smartcard, parameters attached to the second phone number by parameters attached to the first phone number,
- A service-using step, in which a user uses the second smart card with parameters attached to the first smartcard.

Generally, the invention is based on a secure message based process.

In the drawing:

Figure 1 is a diagrammatic view of the architecture to which the invention can be applied, This figure also shows the different steps performed during the process.

Solution description

In our illustrated example, the portable object will be illustrated as a mobile phone.

Consider a subscriber who wishes to replace his / her SIM card A (with $IMSI_A$, Ki_A assigned to $MSISDN_A$). He / she purchases (or is given by the operator under some promotion / loyalty scheme) a new SIM card ($IMSI_B$, Ki_B). The new SIM card B, might (or might not) have an assigned mobile number ($MSISDN_B$). In any case, this solution envisages new cards with pre-assigned mobile numbers.

If the subscriber wishes to retain his old number on card B, the solution takes care of the requirement as represented on figure 1. Figure 1 represents an example of a system to which the invention can be applied.

In our example, the system comprises the following elements –

SIM card SCA – the old card that the user wants to change. It contains, amongst
other data, $IMSI_A$ Ki_A which enable access to the network, and ADM Key_A – administrative keys that allow update of data present in the card. On the network (HLR, AuC, Billing System, etc.), $MSISDN_A$ is assigned to card SCA.

SIM card SCB - the new card that the user wants to use. It contains, amongst other data, $IMSI_B$ Ki_B which enable access to the network, and ADM Key_B –

administrative keys that allow update of data present in the card. On the network (HLR, AuC, Billing System, etc.), $MSISDN_B$ is assigned to card SCB.

Application server AS – In our example, this platform incorporates OTA functionalities, ie, the mechanism to send an APDU (embedded in a special SMS) to the card. When such an SMS is received by the SIM card, it is interpreted accordingly and the embedded APDU is implemented by the card's operating system. In the present case, the embedded instructions include – verify key, update file data, etc. The platform also has a module to interface securely with network elements (HLR, Billing System, etc.) for getting details of cards SCA &SC B.

In our illustrated example, the process is the following (each step is identified by a number which is also visible on figure 1):

1. With card SCA in the mobile, the subscriber sends a SMS containing the mobile number ($MSISDN_B$) assigned to card SCB. The message is sent to a pre-defined number assigned to an Application server AS.
   To illustrate - the subscriber simply goes to the "Messages" option on his / her mobile phone, types in a field, the $MSISDN_B$, and sends the corresponding SMS to the number assigned to the Application server AS. All these steps could be printed on a brochure / flyer given along with new SIM card SCB, and the subscriber simply follows the instructions. A need for Step 1, is to make sure that
   - the user (who has bought the new card) is initiating the process,
   - the new card SCB is a valid replacement card,
   - And finally, to get the details of the 2 cards on which the operation is to be performed.

2. Using information obtained from the origin ($MSISDN_A$) and content ($MSISDN_B$) of the SMS, the application server AS requests the network for details corresponding to cards SCA and SCB. These details include $IMSI_A$ Ki_A ADM Key_A and $IMSI_B$ Ki_B ADM Key_B corresponding respectively to $MSISDN_A$ and MSISDNB.
Depending on the network architecture & data policy, the Application Server, AS could be interfaced with one or several network elements (HLR, Billing System, AuC). Or else, and if possible, the AS could get details of SCA and SCB from a separate database on SIM cards that is maintained by the operator for administrative purposes.

3. Using ADM KeyA the Application server sends an encrypted SMS to MSISDNA (card SCA) which destroys IMSIA KiA in the card. 1 More specifically, this would imply updating IMSI and Ki values with data that is impertinent to the network. For all practical purposes, this would render the card unusable.
On the subscriber side, the message could be : « Now insert new card in handset . »
Generally, in OTA messages, there are 3 levels of security
- Signature (the sending entity should be acceptable by the card),
- Encryption
- and synchronization (there is an incrementing synchro counter in the card, and the card will accept a special OTA message only if it contains the right synchro count).

Depending on operator requirements, we could incorporate all or any of these features. Encryption is required particularly for end to end security. IMSI - Ki values being sensitive data, in our illustrated example, the operator might seek assurance on data integrity. On the card side, the necessary

algorithm shall be embedded to allow processing (decryption) of encrypted messages received from the Application Server, AS.

4. The subscriber takes out card SCA, and inserts card SCB in the phone. He / she now logs on to the network with the mobile number (MSISDNB) assigned to card SCB. Using ADM KeyB the Application server sends an encrypted SMS to MSISDNB (card SCB) which updates IMSIB KiB values in the card with IMSIA KiA. In addition, ADM KeyB is updated with ADM KeyA and subsequently the card is also « refreshed ». In our example, ADM key is updated to permit future, if any, OTA administration of the card.
   In our implementation, the message sent to card SCB is actually sent at Step 3, at the same time that the message is sent to card SCA. However, card SCB will receive the message only after it has been inserted in the mobile phone.

5. Upon « refresh », the mobile reads the updated values - $IMSI_A$ Ki_A, and logs on to the network with the old phone number ($MSISDN_A$).

In our illustrated example, ADM is updated. Nevertheless, this example is not limitative. Updating ADM is interesting for verifying the ADM key for updating files. Updating ADM can be avoided, by assigning old ADM key (of SCA) to new card SCB, on the network.

Scope of the solution

All GSM operators could use the solution – this in turn represents the potential market for this solution.

In our illustrated example, the solution uses SMS for seamless mobile number retention. This makes it convenient for the user. He could do the operation sitting at home.

PoS (Point of Sale) could also be used. This PoS could be linked to the network via internet (or via a direct phone line) to perform the changes on cards.
According to this example, the subscriber goes to a shop equipped with such a PoS terminal.

Claims

1. Method for managing phone numbers attribution after replacement of a smart card (SCA), particularly a SIM card, by a new smart card (SCB), said smart card (SCA) being coupled to a portable object (PO) being able to communicate with a network, said smart card (SCA) storing at least one parameter ($IMSI_A$, ADM_A, Ki_A) attached to a first current phone number,($MSISDN_A$), characterized in that it comprises the following steps:
   - A service-inserting step, in which the new smart card (SCB) storing at least one parameter ($IMSI_B$, ADM_B, Ki_B) attached to the second phone number ($MSISDN_B$) is inserted in the portable object;
   - A service-replacing step, in which an application server (AS) sends a message (M2) for replacing, in the new smart card (SCB), parameters ($IMSI_B$, ADM_B, Ki_B) attached to the second phone number ($MSISDN_B$) by parameters ($IMSI_A$, ADM_A, Ki_A) attached to the first phone number ($MSISDN_A$);
   - A service-using step, in which the user now uses the second smart card (SCB) with the phone number ($MSISDN_A$) previously attached to the first smart card (SCA).

2. Method according to claim 1, characterized in that, for the service-information step, the portable object (PO), while containing first smart card (SCA), sends a message (M1) to an application server (AS), the message (M1) including at least one parameter (MSISDNB) identifying the phone number assigned to second smart card (SCB), which will be used to replace the first smart card (SCA).

3. Method according to claim 1, characterized in that, before the service-inserting step, the application server (AS) sends a secure message (M3)

for deleting, in the first smart card (SCA), parameters ($IMSI_A$, ADM_A ,Ki_A) attached to the first phone number ($MSISDN_A$).

4. Method according to claim 3, characterized in that the message (M3) is encrypted, the encryption being performed by using an encryption key (belonging to the set of keys ADM_A) attached to the first smart card (SCA), and by using an algorithm that resides both on the Application Server (AS), and on the smart card (SCA).

5. Method according to claim 1, characterized in that, for the service replacing step, the application server (AS) sends a secure message (M3) to the new smart card (SCB).

6. Method according to claim 5, characterized in that the message is encrypted, the encryption being performed by using an encryption key (belonging to the set of keys ADM_B) attached to the new smart card (SCB), and by using an algorithm that resides both on the Application Server (AS), and on the smart card (SCB).

7. Method according to claim 1, characterized in that, for the service using step, the portable object logs on to the network using said new smart card (SCB) and said old parameters ($MSISDN_A$, $IMSI_A$, ADM_A, Ki_A).

8. Method according to claims 1 to 6, characterized in that messages are SMS messages.

Abstract

Method for managing phone numbers attribution after replacement of a smart card (SCA), particularly a SIM card, by a new smart card (SCB), said smart card (SCA) being coupled to a portable object (PO) being able to communicate with a network, said smart card (SCA) storing at least one parameter ($IMSI_A$, ADM_A, Ki_A) attached to a first current phone number,($MSISDN_A$), characterized in that it comprises the following steps:

- A service-inserting step, in which the new smart card (SCB) storing at least one parameter ($IMSI_B$, ADM_B, Ki_B) attached to the second phone number ($MSISDN_B$) is inserted in the portable object;
- A service-replacing step, in which an application server (AS) sends a message (M2) for replacing, in the new smart card (SCB), parameters ($IMSI_B$, ADM_B, Ki_B) attached to the second phone number ($MSISDN_B$) by parameters ($IMSI_A$, ADM_A, Ki_A) attached to the first phone number ($MSISDN_A$);
- A service-using step, in which the user now uses the second smart card (SCB) with the phone number ($MSISDN_A$) previously attached to the first smart card (SCA).

Figure 1.

1/1

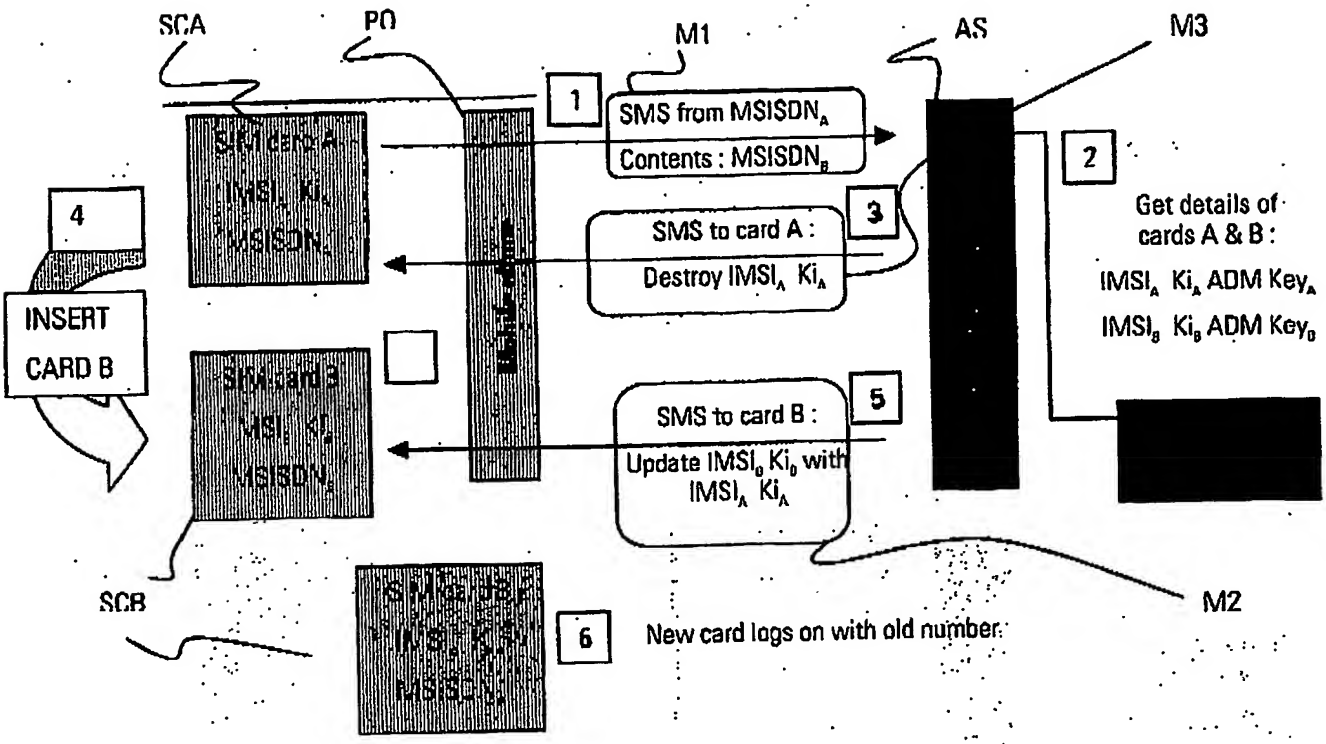
SCA
PO
M1
AS
M3
1
SMS from MSISDN$_A$
Contents : MSISDN$_B$
2
Get details of cards A & B :
IMSI$_A$ Ki$_A$ ADM Key$_A$
IMSI$_B$ Ki$_B$ ADM Key$_B$
3
SMS to card A :
Destroy IMSI$_A$ Ki$_A$
4
INSERT CARD B
5
SMS to card B :
Update IMSI$_B$ Ki$_B$ with IMSI$_A$ Ki$_A$
SCB
6
New card logs on with old number
M2

Figure 1